

05.10.2004

日 本 国 特 許 庁
JAPAN PATENT OFFICE

REC'D 18 NOV 2004

WIPO

PCT

別紙添付の書類に記載されている事項は下記の出願書類に記載されている事項と同一であることを証明する。

This is to certify that the annexed is a true copy of the following application as filed with this Office.

出 願 年 月 日 2 0 0 3 年 1 0 月 1 6 日
Date of Application:

出 願 番 号 特 願 2 0 0 3 - 3 5 6 0 7 2
Application Number:
[ST. 10/C]: [J P 2 0 0 3 - 3 5 6 0 7 2]

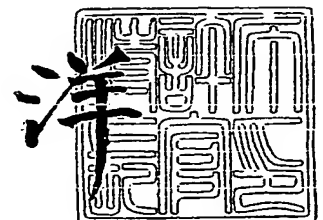
出 願 人 松下電器産業株式会社
Applicant(s):

PRIORITY DOCUMENT
SUBMITTED OR TRANSMITTED IN
COMPLIANCE WITH
RULE 17.1(a) OR (b)

2 0 0 4 年 1 1 月 5 日

特許庁長官
Commissioner,
Japan Patent Office

小 川



【書類名】 特許願
【整理番号】 2022550333
【提出日】 平成15年10月16日
【あて先】 特許庁長官殿
【国際特許分類】 H04M 1/66
【発明者】
 【住所又は居所】 大阪府門真市大字門真 1 0 0 6 番地 松下電器産業株式会社内
 【氏名】 横田 薫
【発明者】
 【住所又は居所】 大阪府門真市大字門真 1 0 0 6 番地 松下電器産業株式会社内
 【氏名】 大森 基司
【特許出願人】
 【識別番号】 000005821
 【氏名又は名称】 松下電器産業株式会社
【代理人】
 【識別番号】 100097445
 【弁理士】
 【氏名又は名称】 岩橋 文雄
【選任した代理人】
 【識別番号】 100103355
 【弁理士】
 【氏名又は名称】 坂口 智康
【選任した代理人】
 【識別番号】 100109667
 【弁理士】
 【氏名又は名称】 内藤 浩樹
【手数料の表示】
 【予納台帳番号】 011305
 【納付金額】 21,000円
【提出物件の目録】
 【物件名】 特許請求の範囲 1
 【物件名】 明細書 1
 【物件名】 図面 1
 【物件名】 要約書 1
 【包括委任状番号】 9809938

【書類名】 特許請求の範囲**【請求項 1】**

携帯端末による記録担体アクセス方法であって、

記録担体へのアクセスを許可する携帯端末の端末 ID リストからなるアクセス許可端末情報を前記記録担体の内部に登録する登録ステップと、

前記携帯端末が前記記録担体に対して、アクセス要求及び前記携帯端末の端末 ID を送付するアクセス要求ステップと、

前記アクセス要求ステップにおいて送付された前記端末 ID と、前記登録ステップにおいて登録したアクセス許可端末情報とを比較して、前記端末 ID が前記アクセス許可端末情報に含まれている場合には、前記携帯端末のアクセス要求を許可し、含まれていない場合には前記アクセス要求を拒否するアクセス許可判断ステップと

を含むことを特徴とする記録担体アクセス方法。

【請求項 2】

前記登録ステップは、

登録用端末に 1 つあるいは 2 つ以上の端末 ID を入力する端末 ID 入力サブステップと、

前記登録用端末が、前記端末 ID 入力ステップにおいて入力された 1 つあるいは 2 つ以上の端末 ID を含む登録要求データを前記記録担体に入力する登録要求データ入力サブステップと、

前記記録担体が、前記登録要求データに含まれる 1 つあるいは 2 つ以上の端末を前記アクセス許可端末情報に追加するアクセス許可端末情報更新サブステップと

を含むことを特徴とする請求項 1 に記載の記録担体アクセス方法。

【請求項 3】

前記登録ステップは、携帯端末に認証コードを入力する認証コード入力ステップと、

前記携帯端末が、前記認証コードと携帯端末自身の端末 ID とからなる登録要求データを前記記録担体に入力する登録要求データ入力ステップと、

前記記録担体が、前記登録要求データに含まれる認証コードと記録担体内部に予め設定されている参照用認証コードとを比較して一致する場合に限り登録要求データに含まれる端末 ID を前記アクセス許可端末情報に追加するアクセス許可端末情報更新ステップと

を含むことを特徴とする請求項 1 に記載の記録担体アクセス方法。

【請求項 4】

前記登録ステップは、サーバーが前記携帯端末に、1 つまたは 2 つ以上の携帯端末の端末 ID を含む登録指示データを送付する登録指示データ送付サブステップと、

前記携帯端末が、前記登録指示データを前記記録担体に送付する登録指示データ転送サブステップと、

前記記録担体が、前記登録データに含まれる 1 つまたは 2 つ以上の端末 ID を、内部に記憶するアクセス許可端末情報に追加するアクセス許可端末情報更新サブステップと

を含むことを特徴とする請求項 1 に記載の記録担体アクセス方法。

【請求項 5】

携帯端末による記録担体アクセス方法であって、

記録担体へのアクセスを許可する携帯端末の端末 ID リストからなるアクセス許可端末情報をサーバーに登録する登録ステップと、

前記携帯端末が前記記録担体に対して、アクセス要求及び前記携帯端末の端末 ID を送付するアクセス要求ステップと、

前記アクセス要求を受けて、前記記録担体が前記携帯端末に対してアクセス許可端末情報を要求するアクセス許可端末情報要求ステップと、

前記アクセス許可端末情報要求ステップを受けて、前記携帯端末が前記サーバーに登録されているアクセス許可端末情報を取得し、前記記録担体に送付するアクセス許可端末情報送付ステップと、

前記アクセス許可端末情報送付ステップを受けて、前記アクセス要求ステップにおいて

送付された前記端末IDと、前記アクセス許可端末情報送付ステップにおいて送付されたアクセス許可端末情報とを比較して、前記端末IDが前記アクセス許可端末情報に含まれている場合には、前記携帯端末のアクセス要求を許可し、含まれていない場合には前記アクセス要求を拒否するアクセス許可判断ステップとを含むことを特徴とする記録担体アクセス方法。

【請求項6】

携帯端末からのアクセスを制御する機能を有する記録担体であって、

外部からのアクセスを制限するアクセス制限領域と、外部からのアクセスを制限しない一般領域とからなるデータ記憶手段と、

前記アクセス制限領域へのデータアクセスを許可する携帯端末の端末IDのデータからなるアクセス許可端末情報を記憶するアクセス許可端末情報記憶手段と、

外部からの登録要求に応じて、前記アクセス許可端末情報記憶手段に記憶するアクセス許可端末情報を更新するアクセス許可端末情報登録手段と、

携帯端末から前記アクセス制限領域へのアクセス要求があった場合に、前記携帯端末の端末IDと前記アクセス許可端末情報記憶手段に記憶するアクセス許可端末情報とを比較して、前記端末IDが前記アクセス許可端末情報に含まれている場合には、前記携帯端末のアクセス要求を許可し、含まれていない場合には前記アクセス要求を拒否するアクセス制御手段と

を備えることを特徴とする記録担体。

【請求項7】

前記アクセス許可端末情報登録手段は、

外部からの登録要求データを受け付ける登録要求データ受付手段と、

認証コードを記憶する認証コード記憶手段と、

前記登録要求データに含まれる認証コードと前記認証コード記憶手段に記憶する認証コードとを比較する認証コード比較手段と、

前記認証コード比較手段によって認証コードが一致すると判断された場合に限り、前記登録要求データに含まれる端末IDを前記アクセス許可端末情報記憶手段に記憶するアクセス許可端末情報に追加するアクセス許可端末情報変更手段と

を備えることを特徴とする請求項6に記載の記録担体。

【請求項8】

前記アクセス許可端末情報登録手段は、

サーバーからネットワークを介して前記携帯端末に送付される登録要求データを受け付ける登録要求データ受付手段と、

前記登録要求データに含まれる端末IDを、前記アクセス許可端末情報記憶手段に記憶するアクセス許可端末情報に追加するアクセス許可端末情報更新手段と

を備えることを特徴とする請求項6に記載の記録担体。

【請求項9】

携帯端末からのアクセスを制御する機能を有する記録担体であって、

前記携帯端末からのアクセス要求及び前記携帯端末の端末IDの送付を受けて、前記携帯端末に対してアクセス許可端末情報を要求するアクセス許可端末情報要求手段と、

サーバーに記録されており、前記携帯端末を介して送付されるアクセス許可端末情報と前記端末IDとを比較して、前記端末IDが前記アクセス許可端末情報に含まれている場合には、前記携帯端末のアクセス要求を許可し、含まれていない場合には前記アクセス要求を拒否するアクセス制御手段と

を備えることを特徴とする記録担体。

【請求項10】

請求項7に記載の記録担体内のデータにアクセスする携帯端末であって、

外部から認証コードの入力を受け付ける認証コード受付手段と、

前記認証コードと携帯端末自身の端末IDとを含む登録要求データを生成する登録要求データ生成手段と、

前記記録担体に前記登録要求データを前記記録担体に送付する登録要求データ送付手段と

を備えることを特徴とする携帯端末。

【請求項 11】

請求項 9 に記載の記録担体内のデータにアクセスする携帯端末であって、

前記記録担体へ、携帯端末自身の端末 ID を含むアクセス要求データを送付するアクセス要求データ送付手段と、

前記記録担体からのアクセス許可端末情報要求を受け付けるアクセス許可端末情報要求受付手段と、

アクセス許可端末情報を蓄積するサーバーからアクセス許可端末情報を受信するアクセス許可端末情報受信手段と、

受信したアクセス許可端末情報を前記記録担体に送付するアクセス許可端末情報送付手段と

を備えることを特徴とする請求項 10 に記載の携帯端末。

【書類名】 明細書

【発明の名称】 記録担体アクセス方法、記録担体、携帯端末装置

【技術分野】

【0001】

本発明は、SIMカードなどのICカードやSDカード、メモリースティック、コンパクトフラッシュ（登録商標）などのメモリカードといった記録担体が装着可能な携帯端末機器及び記録担体に関するものであり、特に記録担体が盗難されたあるいは紛失した場合の対策として、携帯端末機器から記録担体内部のデータへのアクセスを制御する技術に関する。

【背景技術】

【0002】

近年、携帯電話やPDA（Personal Digital Assistant）などの携帯端末の高性能化、高機能化に伴い、SIM（Subscriber Identity Module）カードなどのICカードや、SDカード、メモリースティック、コンパクトフラッシュ（登録商標）などのメモリカードといった記録担体を装着するためのカードスロットを搭載した携帯端末が普及している。

【0003】

それらの記録担体には、自分や知人の氏名、電話番号、メールアドレス、住所などの情報を含んだアドレス帳データや、カメラ付き携帯電話で撮影したデジタル写真データといった、プライベートな情報が記録されている。即ち、記録担体の保有者としては、他人に見られたくない個人情報に属するようなデータを記録担体に記録している。従って、万一その記録担体が盗難されたあるいは紛失した場合であっても、記録しているデータが他人には見られることがないような仕組みが必要になってくる。

【0004】

上記のように記録担体の盗難／紛失に対する対策技術の第1の従来例として、特許文献1に開示されている方法がある。この方法では、記録担体は携帯電話機に装着されるSIMカードを想定している。SIMカードは、携帯電話機の買い替えによる電話番号や登録データなどの移行をスムーズに行うために用いるもので、カードには、電話番号などのIDコードが登録、記録されているとともに、電話帳や着信履歴データが記録されている。買い替えなどにより携帯電話機を別の電話機に交換する場合には、現在の電話機に装着しているSIMカードを新しい携帯電話機に差し替えるだけで、電話番号の移行と電話帳、着信履歴などの個人データの移行が行える。

【0005】

本従来例では、SIMカードを盗んだ第3者がそのSIMカードを自分の電話機に装着して電話をかけることによってその電話料金をSIMカードの持ち主に負わせるような不正使用と電話帳や通話履歴などの個人データを覗き見る行為を防ぐことを目的としている。本従来例によると、SIMカードには前記のID情報、個人データの他に、固有の無効化コードが設定されている点に特徴がある。そして、万一、記録担体が盗難あるいは紛失にあった場合には、前記無効化コードを、前記SIMに装着された携帯電話機に電話をかけることによって送信する。無効化コードを受信した携帯電話機はそれをSIMカードに転送し、受け取ったSIMカードはその無効化コードが予めカード内に記憶しているものと一致するかを確認して一致する場合には、SIMカードのメモリのデータをロックして使用不能状態にする。これによって、他人のSIMカードを用いて電話を掛ける不正使用や、カード内の個人情報覗き見を防止することが可能となる。

【0006】

また、第2の従来例として、カード内のデータを他人の覗き見から守る一般的な方法であるパスワードによるデータロックの方法がある。この方法では、カード内には予めロックを解除するためのパスワードが設定されており、カード内のデータにアクセスするためには、パスワードを入力してロックを解除する必要がある。これにより、万一カードが他人の手に渡ったとしても、パスワードを知らないので他人によるカード内データの漏洩が

防止される。

【特許文献1】特開平11-177682号公報

【発明の開示】

【発明が解決しようとする課題】

【0007】

しかしながら、第1の従来例では、記録担体が外部から送信されるデータの受信が可能な携帯端末に装着されていることによって無効化コード送信によるカードロックが有効に働くことになる。即ち、盗まれた記録担体が、すぐに携帯端末から抜き取られ、オフラインで使用可能なカードデータ読み取り装置によって、カード内の電話帳データや通話履歴などの個人情報が全て抜き取られるような不正は阻止できない。また、近年携帯電話機にスロットが搭載されているSDカードやメモリースティックなどでは、電話帳のみならず、スケジュール帳やカメラ付き携帯電話で撮影したプライベート画像などの多くの個人のプライバシーに関わるデータが記憶されており、第1の従来例の方法をこれらのカードにも適用した場合には、前記オフラインによるカード読み取りによる個人情報流出の被害はより大きいものとなり深刻な問題となる。即ち、前記のようなカード内データの覗き見に対して、第1の従来例は、十分に防止できないという課題がある。

【0008】

また、第2の従来例では、第1の従来例に関する上記のような課題は解決されるものの、正規カード保有者であっても記録担体内のデータにアクセスするたびに、パスワードを入力が要求されることになり、正規カード保有者の操作性を大きく損ねるという課題がある。

【0009】

本発明は、前記従来課題を解決するもので、第2の従来例のように正規カード保有者にとって操作の面で大きな負担をかけず、かつ、第1の従来例の課題としてあげたようなオフライン環境下でのカード内データの覗き見も防止することが可能な記録担体アクセス方法を提供することを目的とする。

【課題を解決するための手段】

【0010】

前記従来課題を解決するために、本発明の記録担体は、外部からのアクセスを制限するアクセス制限領域と、外部からのアクセスを制限しない一般領域とからなるデータ記憶手段と、前記アクセス制限領域へのデータアクセスを許可する携帯端末の端末IDのデータからなるアクセス許可端末情報を記憶するアクセス許可端末情報記憶手段と、外部からの登録要求に応じて、前記アクセス許可端末情報記憶手段に記憶するアクセス許可端末情報を更新するアクセス許可端末情報登録手段と、携帯端末から前記アクセス制限領域へのアクセス要求があった場合に、前記携帯端末の端末IDと前記アクセス許可端末情報記憶手段に記憶するアクセス許可端末情報とを比較して、前記端末IDが前記アクセス許可端末情報に含まれている場合には、前記携帯端末のアクセス要求を許可し、含まれていない場合には前記アクセス要求を拒否するアクセス制御手段とを備える。

【0011】

本構成によって、アクセス許可端末情報に含まれない携帯端末による記録担体へのアクセスを防止することができる。

【発明の効果】

【0012】

本発明の記録担体によれば、正規カード保有者にとって操作の面で大きな負担をかけず、かつ、オフライン環境下でのカード内データの覗き見も防止することができる。また、本発明の記録担体アクセス方法によれば、ユーザーの操作負担を課さずに他人からのデータ覗き見に対する安全性を高めることができる。

【発明を実施するための最良の形態】

【0013】

以下本発明の実施の形態について、図面を参照しながら説明する。

【0014】

(実施の形態1)

図1は、本発明の実施の形態1において、携帯端末2が記録担体1内部のデータにアクセスする場合の構成図である。ここで、携帯端末2としては、携帯電話機などが、記録担体1としては、SDカード、メモリースティックなどのメモリカードや、SIMカードなどのICカードといったものが想定される。また、携帯端末2には記録担体1を装着するためのスロットがあり、記録担体1は前記スロットに装着されているものとする。

【0015】

記録担体1は、携帯端末2とのデータやりとりを行う端末I/F10と、記録担体1内部の動作を制御する制御部11と、記録担体1の内部データにアクセス可能な機器の情報を記憶するアクセス可能機器情報記憶部12と、データを記憶するデータ記憶部13と、アクセス可能機器情報記憶部12にアクセス可能機器情報の登録を行うアクセス可能機器情報登録部15からなる。また、データ記憶部13の内部には、アクセス可能機器情報記憶部12に記憶するアクセス可能機器情報に基づいて、アクセスが制限されるアクセス制限領域14が存在する。さらに、アクセス可能機器情報記憶部12は外部からの直接アクセスができないようになっている。

【0016】

携帯端末2は、記録担体1とのデータやりとりを行う記録担体I/F20と、携帯端末を識別するための端末IDを記憶する端末ID記憶部21と、携帯端末2内部の動作を制御する制御部22と、ユーザーによる携帯端末2外部からの入力を受信する外部入力I/F23と、携帯端末2の内部データをユーザーに見える形にして表示する表示部24からなる。

【0017】

以下、携帯端末2が、記録担体1内のデータ記憶部13にあるアクセス制限領域14に記録されているデータにアクセスする場合の動作について説明する。

【0018】

記録担体1内部のアクセス可能機器情報記憶部12には、後で述べる方法によって既にアクセス可能機器情報が記憶されているものとする。

【0019】

まず、携帯端末2に対してユーザーが記録担体1に記憶する所定データの表示要求を行う。具体的には、携帯端末2に搭載されている所定の入力ボタンを押下することによって行われる。その要求は外部入力I/F23を介して制御部22に伝達される。

【0020】

前記要求を受けた制御部22は、端末ID記憶部21に記憶する端末IDを読み出して、データアクセス要求とともに記録担体I/F20を介して記録担体1に送信される。ここで端末IDは各携帯端末を識別するための識別情報であり、例えば携帯電話の電話番号や、端末のシリアル番号などのようなものでよい。

【0021】

前記データアクセス要求と端末IDは記録担体1内部の端末I/F10にて受信され、制御部11に転送される。制御部11は、アクセス可能機器情報記憶部12に記憶されるアクセス可能機器情報を元に携帯端末2のデータアクセス要求を許可するかどうかを判断する。具体的には、前記アクセス可能機器情報は、記録担体1内部のアクセス制限領域14にアクセス可能な携帯端末の端末IDのリストからなり、制御部11は、携帯端末2から送付されてきた端末IDが前記リストの中に存在するかどうかをチェックしてアクセス要求を許可するかどうかを決定する。前記判断の結果、アクセス要求を許可する場合には、制御部11は、データ記憶部13内のアクセス制限領域14の中から携帯端末2から要求されているデータを取得して、端末I/F10を介して携帯端末2に送付する。アクセス要求を許可しない場合には、アクセス許可された端末でない旨を知らせる情報を端末I/F10を介して携帯端末2に送付する。

【0022】

記録担体 1 から前記データを受信した携帯端末 2 は、記録担体 I/F 20 を介して制御部 22 に転送される。制御部 22 は、受信したデータの内容を確認して、ユーザーが要求したデータである場合には、そのデータの内容を表示部 24 に表示してユーザーに情報を提供する。一方、レスポンスのデータがアクセス許可された端末でない旨を知らせる内容である場合には、表示部 24 にこの携帯端末が要求されたデータにアクセスすることを許可されていないことを示すメッセージを表示させる。

【0023】

次に、アクセス可能機器情報記憶部 12 にアクセス可能機器情報を記憶／更新する方法について説明する。

【0024】

図 2 は、本発明の実施の形態 1 においてアクセス可能機器情報記憶部 12 にアクセス可能機器情報を記憶／更新するための第 1 の方法に関する機器構成を示したものである。図 2 において、記録担体 1 は、図 1 に示す記録担体 1 と同一のものである。アクセス可能機器情報登録器 3 は、記録担体 1 内部のアクセス可能機器情報記憶部 12 にアクセス可能機器情報を登録するための専用機器であり、機器外部から端末 ID の入力を受け付けて書き込み許可データ生成部 31 に転送する外部入力 I/F 30 と、外部入力 I/F 30 から転送された端末 ID データを元に、アクセス可能機器情報登録指示データを作成して記録担体 I/F 32 に転送する書き込み許可データ生成部 31 と、前記アクセス可能機器情報登録指示データを記録担体 1 に転送する記録担体 I/F 32 からなる。本実施の形態において、アクセス可能機器情報の登録は、登録処理が認められた専用の機器（即ち、アクセス可能機器情報登録器 3 のような専用機器）以外では行うことができないものとする。また、アクセス可能機器情報登録器 3 は記録担体 1 を装着するためのスロットを有しており、記録担体 1 はこのスロットに装着された状態で以下の動作が行われるものとする。

【0025】

以下、アクセス可能機器情報登録器 3 を用いて記録担体 1 にアクセス可能機器情報を記憶／更新する際の動作について説明する。

【0026】

まず、記録担体 1 にアクセス可能機器を登録する処理なのか、あるいは、既に登録されているアクセス可能機器の登録削除を行う処理なのかを示す登録／登録削除指示データと、登録あるいは登録削除を行う対象となる携帯端末の端末 ID がアクセス可能機器情報登録器 3 に外部から入力される。このとき、登録あるいは登録削除する端末 ID は 1 つである必要はなく、1 度の処理で複数の端末 ID を入力してもよい。外部から入力される登録／登録削除指示データと端末 ID は外部入力 I/F 30 で受け付けられ、外部入力 I/F 30 は、入力された端末 ID を書き込み許可データ生成部 31 に転送する。次に、書き込み許可データ生成部 31 は、入力された登録／登録削除指示データと端末 ID をもとに記録担体処理データを作成する。記録担体処理データの具体内容としては、アクセス可能機器情報記憶部 12 への端末 ID 登録／登録削除を指示するためのコマンドコードと、そのコマンドコードの実行によって登録／登録削除を行う端末 ID の個数と、登録／登録削除を行う端末 ID のリストを結合したデータ列からなる。この記録担体処理データは記録担体 I/F 32 を介して記録担体 1 に送付される。

【0027】

前記記録担体処理データは、記録担体 1 内部の端末 I/F 10 で受け付けられて、アクセス可能機器情報登録部 15 に転送される。アクセス可能機器情報登録部 15 は、入力された記録担体処理データを解釈して、アクセス可能機器情報記憶部 12 に記憶しているアクセス可能機器情報の更新を行う。具体的には、アクセス可能機器の登録を行う指示のデータを受け取った場合には、データが指定する端末 ID をアクセス可能機器情報に追加する。このとき、指定する端末 ID が既にアクセス可能機器情報として登録済みの場合には、アクセス可能機器情報登録器 3 にその旨のエラーメッセージを返す。また、アクセス可能機器の削除を行う指示のデータを受け取った場合には、データが指定する端末 ID をアクセス可能機器情報から削除する。このとき、指定する端末 ID がアクセス可能機器情報

に登録されていない場合には、アクセス可能機器情報登録器 3 にその旨のエラーメッセージを返す。上記の一連の処理によってアクセス可能機器情報記憶部 12 に記憶するアクセス可能機器情報が更新される。

【0028】

このとき、アクセス可能機器情報の不正規な登録／削除処理が記録担体 1 に対して行われるのを避けるために、以下のような処理を追加してもよい。即ち、アクセス可能機器情報登録器 3 は、公開鍵暗号方式を用いたデジタル署名方式の署名鍵を秘密に保持し、書き込み許可データ生成部 31 は生成した記録担体処理データに前記署名鍵を用いてデジタル署名を施した上で記録担体 1 に送付する。一方、記録担体 1 は、前記署名を検証するための検証鍵を保持しており、アクセス可能機器情報登録部 15 は、前記記録担体処理データの指示に従った処理を行う前に、前記検証鍵を用いて記録担体処理データに施されたデジタル署名の正当性を検証する。このとき、署名の正当性が確認された場合にのみ、その記録担体処理データが正規のアクセス可能機器情報登録器から発行されたデータであると判断して登録／登録処理を継続する。一方、デジタル署名の正当性が確認できなかった場合には、その記録担体処理データを不正なものとして以降の処理を行わないようにする。

【0029】

また、過去の登録／登録削除処理に使用された記録担体処理データを保存しておいて、それを再び記録担体に送付して登録／登録削除処理を実行させるような不正対策、及び、不正規のアクセス可能機器情報登録器による登録／登録削除処理を防止する手段として以下のような処理を追加してもよい。即ち、前記の追加処理と同様に、アクセス可能機器情報登録器 3 には署名鍵、記録担体 1 にはそれに対応する検証鍵を保持しておく。そして、前記の登録／登録削除処理を行う際には、次のステップからなるチャレンジレスポンス認証を行う。

【0030】

1. 記録担体 1 が、乱数を発生してアクセス可能機器情報登録器 3 に送付する
2. アクセス可能機器情報登録器 3 が、前記乱数に対して署名鍵を用いて署名を施して記録担体 1 に返送する
3. 記録担体 1 が、検証鍵を用いて前記署名を検証する
3. において、署名が正当であると確認できたときに限り、登録／登録削除処理を継続し、正当であると確認できなかった場合には登録／登録削除処理を行わない。これによって、正規のアクセス可能機器情報登録器のみが登録／登録削除処理を行え、かつ、同時に不正規登録器が過去の記録担体処理データを再送付して登録／登録削除処理を行うことを防止している。

【0031】

次に、アクセス可能機器情報を登録する第 2 の方法について説明する。図 3 は、本発明の実施の形態 1 におけるアクセス可能機器情報記憶部 12 にアクセス可能機器情報を登録する第 2 の方法に関する機器構成を示したものである。図 3 において、記録担体 1 及び携帯端末 2 は、図 1 に示す記録担体 1 及び携帯端末 2 と同一のものである。以下は、記録担体 1 に対して携帯端末 2 をアクセス可能機器として登録あるいは登録削除する場合の動作について説明している。また、以下の動作は記録担体 1 が携帯端末 2 に装着されている状態で行われるものとする。

【0032】

記録担体 1 には、予め所定のパスワードが設定されアクセス可能機器情報記憶部 12 に記憶されているものとする。これは、例えば、記録担体製造または出荷時にカード固有のパスワードが設定されており、パッケージの箱を開けることで初めて見ることでできる個所にパスワード情報を印刷するなどして、記録担体の購入者のみに知らせるようにすれば良い。

【0033】

まず、携帯端末 2 に対して記録担体 1 に設定されているパスワードと、登録／登録削除指示データとが外部から入力される。入力された前記データは、携帯端末 2 内部の外部入

力I/F23で受け付けて制御部22に転送される。制御部22は、前記入力データに、端末ID記憶部21が記憶する携帯端末2の端末IDを付加した上で、記録担体I/F20を介して記録担体1に送付する。即ち、パスワードと、登録/登録削除指示データと、携帯端末2の端末IDが記録担体1に送付される。このデータは、記録担体1内部の端末I/F10で受け付けて、アクセス可能機器情報登録部15に入力される。

【0034】

次に、アクセス可能機器情報登録部15は、前記入力データに含まれるパスワードがアクセス可能機器情報記憶部12に記憶している記録担体1のパスワードと一致するかを確認し、一致する場合には、以下の処理を行う。一致しない場合には、処理を行わない。前記パスワード確認の後、入力データに含まれる登録/登録削除指示データとその処理対象となる端末IDに従って、アクセス可能機器情報記憶部12に記憶するアクセス可能機器情報を更新する。このとき、アクセス可能機器情報を登録する第1の方法の説明でも述べたように、既に登録済みの端末IDの登録指示である場合、あるいは、登録されていない端末IDの登録削除指示である場合には、その旨のエラーメッセージを携帯端末2に返す。また、携帯端末2から送られてくるパスワード、登録/登録削除指示データ、端末IDが記録担体に送付される過程において改ざんされるのを防止するために、前記第1の方法の場合と同様にして、前記データに対して携帯端末2内部の制御部22でデジタル署名を施し、記録担体1内部のアクセス可能機器情報登録部15で前記デジタル署名の正当性を検証するようにしてもよい。

【0035】

さらに、アクセス可能機器情報を登録する第3の方法について説明する。第3の方法では、記録担体へのアクセス可能機器情報登録/登録削除依頼をアクセス可能機器情報配信サーバー4に対して行い、前記サーバーは、その受け付けた依頼内容に基づいて記録担体1に対してアクセス可能機器情報の更新処理を行う。このとき、サーバーと記録担体は携帯端末2を介してネットワーク経由で前記更新処理を行う。図4は、本発明の実施の形態1におけるアクセス可能機器情報記憶部12にアクセス可能機器情報を登録する第3の方法に関する機器構成を示したものである。

【0036】

図4において、携帯端末2は、図1に示す携帯端末2において、ネットワーク経由でデータの送受信を行う通信I/F25が追加された構成となっている。記録担体1は、図1に示す記録担体1において、各記録担体に固有のID番号(カードID)を記憶するカードID記憶部16が追加された構成となっている。また、アクセス可能機器情報配信サーバー4は、ユーザーからのアクセス可能機器情報登録/登録削除依頼を受けてネットワーク経由で記録担体に記憶するアクセス可能機器情報の更新を行うものであり、外部からの入力データを受け付けて書き込み許可データ生成部41に転送する外部入力I/F40と、前記入力データをもとに記録担体1に送付するための書き込み許可データを生成してデータ送信部42に転送する書き込み許可データ生成部41と、前記書き込み許可データを携帯端末2にネットワーク経由で送付するデータ送信部42からなる。以下、アクセス可能機器情報登録/登録削除を行う際の動作について説明する。なお、以下の動作は記録担体1が携帯端末2に装着された状態で行われるものとする。

【0037】

まず、アクセス可能機器情報配信サーバー4に、依頼データが入力される。依頼データは具体的には、アクセス可能機器情報の登録あるいは登録削除のどちらを行うのかを示す登録/登録削除指示データと、登録/登録削除を行う端末IDと、登録/登録削除を行う対象となる記録担体のカードIDと、本依頼データに基づく登録/登録削除を指示する書き込み許可データの送付先携帯端末を示す送付先データからなる。

【0038】

送付先データの具体的な内容としては、携帯端末2が携帯電話などの場合には電話番号、メール受信機能のある端末の場合にはメールアドレス、IP接続可能な端末の場合にはIPアドレスなどが考えられる。

【0039】

入力された前記依頼データは、外部入力 I/F 40 で受け付けて書き込み許可データ生成部 41 に転送される。前記入力を受けて、書き込み許可データ生成部 41 は、前記依頼データを元に書き込み許可データを生成してデータ送信部 42 に転送する。書き込み許可データは、具体的には、書き込み許可データの送信先を示す送付先データと、本書き込み許可データに含まれる端末 ID の登録/登録削除処理をどの記録担体に対して指示しているのかを示すカード ID と、登録/登録削除のどちらを指示するのかを示す登録/登録削除指示データと、登録/登録削除を行う端末 ID の情報を含んでいる。データ送信部 42 は、前記書き込み許可データに含まれる送付先データが指定する携帯端末 2 に書き込み許可データを送信する。

【0040】

前記書き込み許可データは携帯端末 2 内部の通信 I/F 25 にて受信し、制御部 22 に転送する。さらに制御部 22 は、前記書き込みデータを記録担体 I/F 20 を介して記録担体 1 に送付する。

【0041】

記録担体 1 に送付された書き込み許可データは、端末 I/F 10 にて受信し、アクセス可能機器情報登録部 15 に転送する。アクセス可能機器情報登録部 15 は、まず入力された書き込み許可データに含まれるカード ID とカード ID 記憶部 16 に記憶される記録担体 1 のカード ID とが一致することを確認する。もしも一致しない場合には、本書き込み許可データが記録担体 1 に対して発行されたものではない旨のエラーメッセージを携帯端末 2 に返して処理を終了する。一致する場合は、以下の処理を続行する。次に、書き込み許可データに含まれる、登録/登録削除指示データと端末 ID に従って、アクセス可能機器情報記憶部 12 に記憶するアクセス可能機器情報を更新する。このとき、アクセス可能機器情報を登録する第 1、第 2 の方法の説明でも述べたように、既に登録済みの端末 ID の登録指示である場合あるいは、登録されていない端末 ID の登録削除指示である場合には、その旨のエラーメッセージを携帯端末 2 に返すようにしてもよい。また、書き込み許可データが、アクセス可能機器情報配信サーバー 4 から携帯端末 2 経由で記録担体 1 に送付される過程における改ざん、及び、偽造された書き込み許可データが記録担体 1 に送付され処理されるのを防止するために、前記第 1、第 2 の方法の場合と同様にして、アクセス可能機器情報配信サーバー 4 はデジタル署名生成用の署名鍵を秘密に保持して、内部の書き込み許可データ生成部 41 において生成した書き込み許可データに対してデジタル署名を施して送付するようにしてもよい。このとき記録担体 1 内部では前記デジタル署名を検証するための検証鍵を保持して、アクセス可能機器情報登録部 15 で前記デジタル署名の正当性を検証する。

【0042】

また、過去の登録/登録削除処理に使用された記録担体処理データを保存しておいて、それを再び記録担体 1 に送付して登録/登録削除処理を実行させるような不正対策として以下のような処理を追加してもよい。即ち、前記の追加処理と同様に、アクセス可能機器情報配信サーバー 4 には署名鍵、記録担体 1 にはそれに対応する検証鍵を保持しておく。そして、前記の登録/登録削除処理を行う際には、次のステップからなるチャレンジレスポンス認証を行う。

【0043】

1. 記録担体 1 が、乱数を発生してアクセス可能機器情報配信サーバー 4 に送付する
2. アクセス可能機器情報配信サーバー 4 が、前記乱数に対して署名鍵を用いて署名を施して記録担体 1 に返送する
3. 記録担体 1 が、検証鍵を用いて前記署名を検証する
3. において、署名が正当であると確認できたときに限り、登録/登録削除処理を継続し、正当であると確認できなかった場合には登録/登録削除処理を行わない。これによって、正規のアクセス可能機器情報配信サーバーのみが登録/登録削除処理を行えるので、不正規のアクセス可能機器情報配信サーバーあるいは携帯端末が過去の記録担体処理デー

タを再送付して登録／登録削除処理を行うことを防止できる。

【0044】

かかる構成によれば、記録担体にアクセス可能な端末の端末IDを記録担体内部に保持することにより、携帯端末がネットワークに接続していないオフラインの状態であっても、アクセス可能な端末として登録されていない携帯端末によるアクセスを拒絶する。これによって、第1の従来例では可能であったオフラインの状態でのカードの不正使用を阻止することができ、かつ、第2の従来例のようにカードにアクセスするたびにパスワードの入力を要求するというようなユーザー負担をなくすることができる。

【0045】

(実施の形態2)

実施の形態1では、記録担体へのアクセス許可／拒絶を判断するためのアクセス可能機器情報をその記録担体自身の内部に記録していた。実施の形態2は、アクセス可能機器情報をネットワーク上に存在するアクセス可能機器情報を蓄積配信するためのサーバーに記憶するところに特徴がある。携帯端末からのアクセス要求が来ると、その都度、記録担体は前記サーバーからアクセス可能機器情報を取得してアクセス許可／拒絶の判断を行う。以下、その詳細について説明する。

【0046】

図5は、本発明の実施の形態2において、携帯端末6が記録担体5内部のデータにアクセスする場合の構成図である。このとき、記録担体5は、アクセス可能機器情報管理サーバー7から送られるアクセス可能機器情報に基づいて、携帯端末6によるデータアクセスを許可するかどうかを判断する。

【0047】

記録担体5は、携帯端末6とのデータやりとりを行う端末I/F50と、記録担体5内部の動作を制御する制御部51と、アクセス可能機器情報管理サーバー7から送られてくるアクセス可能機器情報が改ざんされていないかをチェックするアクセス可能機器情報改ざん検査部52と、データを記憶するデータ記憶部53と、記録担体5ごとに固有のID番号であるカードIDを記憶するカードID記憶部55からなる。また、データ記憶部53の内部には、アクセス可能機器情報管理サーバー7から送られてくるアクセス可能機器情報に基づいて、アクセスが制限されるアクセス制限領域54が存在する。

【0048】

携帯端末6は、記録担体5とのデータやりとりを行う記録担体I/F60と、携帯端末6を識別するための端末IDを記憶する端末ID記憶部61と、携帯端末6内部の動作を制御する制御部62と、ユーザーによる携帯端末6外部からの入力を受信する外部入力I/F63と、携帯端末6の内部データをユーザーに見える形にして表示する表示部64と、ネットワーク経由でデータの送受信を行う通信I/F65からなる。

【0049】

アクセス可能機器情報管理サーバー7は、各記録担体のアクセス可能機器情報を記憶するアクセス可能機器情報記憶部70と、アクセス可能機器情報記憶部70に記憶するアクセス可能機器情報の更新を行うアクセス可能機器情報登録部71からなる。

【0050】

以下、携帯端末6が、記録担体5内のデータ記憶部53にあるアクセス制限領域54に記録されているデータにアクセスする場合の動作について説明する。なお、携帯端末6には記録担体5を装着するためのスロットがあり、以下の動作では記録担体5が携帯端末6のスロットに装着された状態で行われるものとする。

【0051】

アクセス可能機器情報管理サーバー7には、予めデジタル署名用の署名鍵が秘密に保持されているものとする。また、前記デジタル署名を検証するための検証鍵が記録担体5内部のアクセス可能機器情報改ざん検査部52に記憶されているものとする。さらに、アクセス可能機器情報管理サーバー7内部のアクセス可能機器情報記憶部70には、後で述べる方法によって記録担体ごとのアクセス可能機器情報が記憶されているものとする。まず

、携帯端末6に対してユーザーが記録担体5に記憶する所定データの表示要求を行う。具体的には、携帯端末6に搭載されている所定の入力ボタンを押下することによって行われる。その要求は外部入力I/F63を介して制御部62に伝達される。

【0052】

前記要求を受けた制御部62は、端末ID記憶部61に記憶する端末IDを読み出して、データアクセス要求とともに記録担体I/F60を介して記録担体5に送信される。ここで端末IDは各携帯端末を識別するための情報であり、例えば携帯電話の電話番号や、端末のシリアル番号などのようなものである。

【0053】

前記データアクセス要求と端末IDは記録担体5内部の端末I/F50で受信され、制御部51に転送される。上記データを受け取った制御部51は、カードID記憶部55に記憶する記憶担体5のカードIDを読み出した後、携帯端末6を経由してアクセス可能機器情報管理サーバー7に対して前記カードIDを送付し、送付したカードIDに対応するアクセス可能機器情報の送付を要求する。前記要求を受けたサーバー7は、アクセス可能機器情報記憶部70において、受け取ったカードIDに対応するアクセス可能機器情報を検索して取り出し、さらに取り出したアクセス可能機器情報に対して署名鍵を用いてデジタル署名を施したものを携帯端末6経由で記録担体5に送付する。

【0054】

前記アクセス可能機器情報を受け取った制御部51は、アクセス可能機器情報改ざん検査部52において、検証鍵を用いてアクセス可能機器情報に施されたデジタル署名の正当性を検証し、正当と判断された場合に限り以下の処理を続行する。正当でないと判断された場合には、その旨のエラーメッセージを携帯端末6に返して処理を中止する。また、前記アクセス可能機器情報の送付要求後、一定の時間が経過してもアクセス可能機器情報が受信されない場合にも、その旨のエラーメッセージを返して処理を中止する。

【0055】

次に、正当性の検証できたアクセス可能機器情報を元に携帯端末6のデータアクセス要求を許可するかどうかを判断する。具体的には、前記アクセス可能機器情報は、記録担体5内部のアクセス制限領域54にアクセス可能な携帯端末の端末IDのリストからなり、制御部51は、携帯端末6から送付されてきた端末IDが前記リストの中に存在するかどうかをチェックしてアクセス要求を許可するかどうかを決定する。前記判断の結果、アクセス要求を許可する場合には、制御部51は、データ記憶部53内のアクセス制限領域54の中から携帯端末6から要求されているデータを取得して、端末I/F50を介して携帯端末6に送付する。アクセス要求を許可しない場合には、アクセス許可された端末でない旨を知らせるデータを端末I/F50を介して携帯端末6に送付する。

【0056】

記録担体5から前記データを受信した携帯端末6は、記録担体I/F60を介して制御部62に転送される。制御部62は、受信したデータの内容を確認して、ユーザーが要求したデータである場合には、そのデータの内容を表示部64に表示してユーザーに情報を提供する。一方、受信したデータがアクセス許可された端末でない旨を知らせるものである場合には、表示部64にこの携帯端末が要求されたデータにアクセスすることを許可されていないことを示すメッセージを表示させる。

【0057】

次に、アクセス可能機器情報管理サーバー7内部のアクセス可能機器情報記憶部70にアクセス可能機器情報を登録/更新する方法について説明する。

【0058】

図6は、本発明の実施の形態2におけるアクセス可能機器情報管理サーバー7内部のアクセス可能機器情報記憶部70にアクセス可能機器情報を登録/更新する方法に関する機器構成を示したものである。図6において、アクセス可能機器情報管理サーバー7は、図5に示すものと同一のものである。ユーザー端末8は、ネットワーク経由でアクセス可能機器情報管理サーバー7にアクセスしてアクセス可能機器情報の登録/更新を行うための

端末であるが、専用端末である必要はなく、例えばネットワーク接続可能なPCや、携帯電話、PDAのようなものであってもよい。以下ユーザー端末8を用いてアクセス可能機器情報の登録／更新を行う際の動作を説明する。

【0059】

ユーザーは予めアクセス可能機器情報管理サーバー7にユーザー名とユーザーパスワードを登録しておく。

【0060】

まずユーザー端末8がアクセス可能機器情報管理サーバー7に接続する際に、前記ユーザー名とユーザーパスワードがユーザー端末8に入力される。前記入力データは、外部入力I/F80、制御部81、通信I/F82を介してアクセス可能機器情報管理サーバー7に送信され、アクセス可能機器情報管理サーバー7は、受け取ったユーザー名とユーザーパスワードが登録されているものと一致することを確認し、一致するときに限り以下の処理を続行する。一致しない場合には処理を中止する。

【0061】

次に、ユーザー端末8に、アクセス可能機器情報を登録／登録削除したい記録担体のカードID、アクセス可能機器情報の登録あるいは登録削除を指示するための登録／登録削除指示データ、及び登録／登録削除したい携帯端末の端末IDからなる依頼データを入力する。入力された依頼データは外部入力I/F80で受け付けて、制御部81、通信I/F82を介してアクセス可能機器情報管理サーバー7に送信される。

【0062】

アクセス可能機器情報管理サーバー7で受信した前記依頼データは、アクセス可能機器情報登録部71にて処理される。具体的には、依頼データに含まれるカードIDに対応するアクセス可能機器情報をアクセス可能機器情報記憶部70に記憶するデータから検索して取り出し、登録／登録削除指示データの指示に従って、指定される端末IDの登録あるいは登録削除を行い、前記取り出したアクセス可能機器情報を更新して再びアクセス可能機器情報記憶部70に記憶する。このとき、依頼データに基づく指示が既にアクセス可能機器情報に登録されている端末IDの登録処理である場合、あるいは、アクセス可能機器情報に登録されていない端末IDの登録削除処理である場合、もしくは、ユーザーが所有していないはずのカードIDに対する登録／登録削除処理である場合には、その旨を示すエラーメッセージをユーザー端末8に返す。

【0063】

かかる構成によれば、アクセス可能機器情報をサーバーに記憶／管理して、携帯端末が記録担体にアクセスする際には、記録担体はサーバーからアクセス可能機器情報の取得を要求して、取得したアクセス可能機器情報に基づいて携帯端末のアクセスを制御する。また、アクセス可能機器情報の取得に失敗した場合には携帯端末のアクセスを拒絶する。これにより、携帯端末がネットワークに接続していないオフラインの状態では、記録担体へのアクセスができないので、第1の従来例では可能であったオフラインの状態でのカードの不正使用を阻止することができ、かつ、第2の従来例のようにカードにアクセスするたびにパスワードの入力を要求するというようなユーザー負担をなくすことができた。

【0064】

さらに、本実施形態では、記録担体とともにアクセス可能機器情報に登録されている携帯端末までもが盗まれるあるいは紛失した場合であっても、ユーザーはユーザー端末を用いてアクセス可能機器情報から前記携帯端末の端末IDを登録削除すれば記録担体の不正使用を阻止できるというメリットもある。

【産業上の利用可能性】**【0065】**

本発明にかかる記録担体は、記録担体の盗難／紛失時の不正利用に対する安全性を高めつつユーザー側の処理負荷は増加させないという効果を有するので、例えば個人情報や金銭データなどを記憶したICカードなどに適用可能である。また、前記の例に限らず、不正使用されたくない重要なデータを記録するメモリカードであれば何でも適用が可能であ

る。

【図面の簡単な説明】

【0066】

【図1】本発明の実施の形態1に係る記録担体アクセス時の記録担体1及び携帯端末2の構成を示すブロック図

【図2】本発明の実施の形態1に係るアクセス可能機器情報登録時の第1の方法における記録担体1及びアクセス可能機器情報登録器3の構成を示すブロック図

【図3】本発明の実施の形態1に係るアクセス可能機器情報登録時の第2の方法における記録担体1及び携帯端末2の構成を示すブロック図

【図4】本発明の実施の形態1に係るアクセス可能機器情報登録時の第3の方法における記録担体1、携帯端末2、及びアクセス可能機器情報配信サーバー4の構成を示すブロック図

【図5】本発明の実施の形態2に係る記録担体アクセス時の記録担体5、携帯端末6、及びアクセス可能機器情報管理サーバー7の構成を示すブロック図

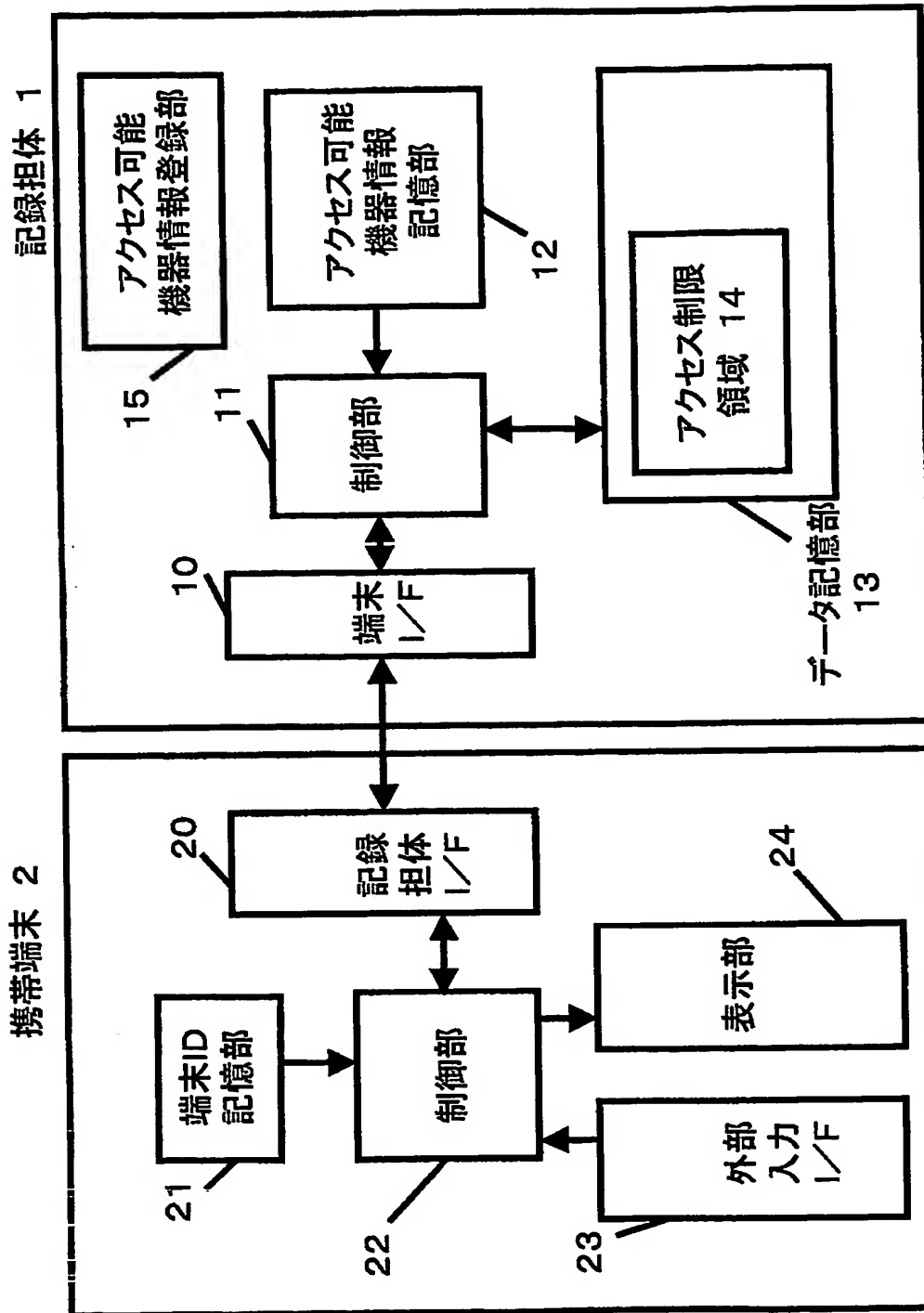
【図6】本発明の実施の形態2に係るアクセス可能機器情報登録時のアクセス可能機器情報配信サーバー7及びユーザー端末8の構成を示すブロック図

【符号の説明】

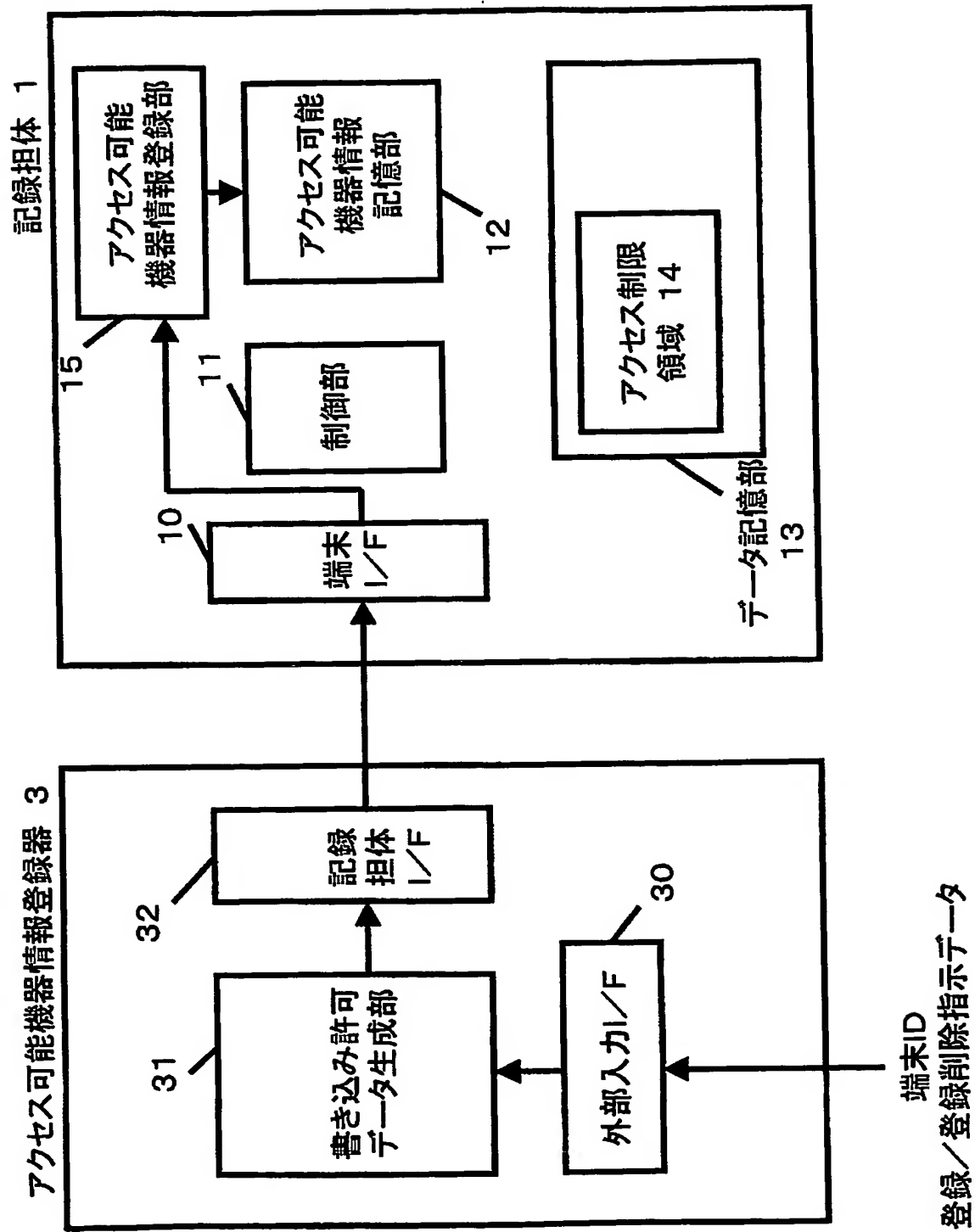
【0067】

- 1, 5 記録担体
- 2, 6 携帯端末
- 3 アクセス可能機器情報登録器
- 4 アクセス可能機器情報配信サーバー
- 7 アクセス可能機器情報管理サーバー
- 8 ユーザー端末
- 10, 50 端末I/F
- 11, 22, 51, 62, 81 制御部
- 12, 70 アクセス可能機器情報記憶部
- 13, 53 データ記憶部
- 14, 54 アクセス制限領域
- 15, 71 アクセス可能機器情報登録部
- 16, 55 カードID記憶部
- 20, 32, 60 記録担体I/F
- 21, 61 端末ID記憶部
- 23, 30, 40, 63, 80 外部入力I/F
- 24, 64 表示部
- 25, 65, 82 通信I/F
- 31, 41 書き込み許可データ生成部
- 42 データ送信部
- 52 アクセス可能機器情報改ざん検査部

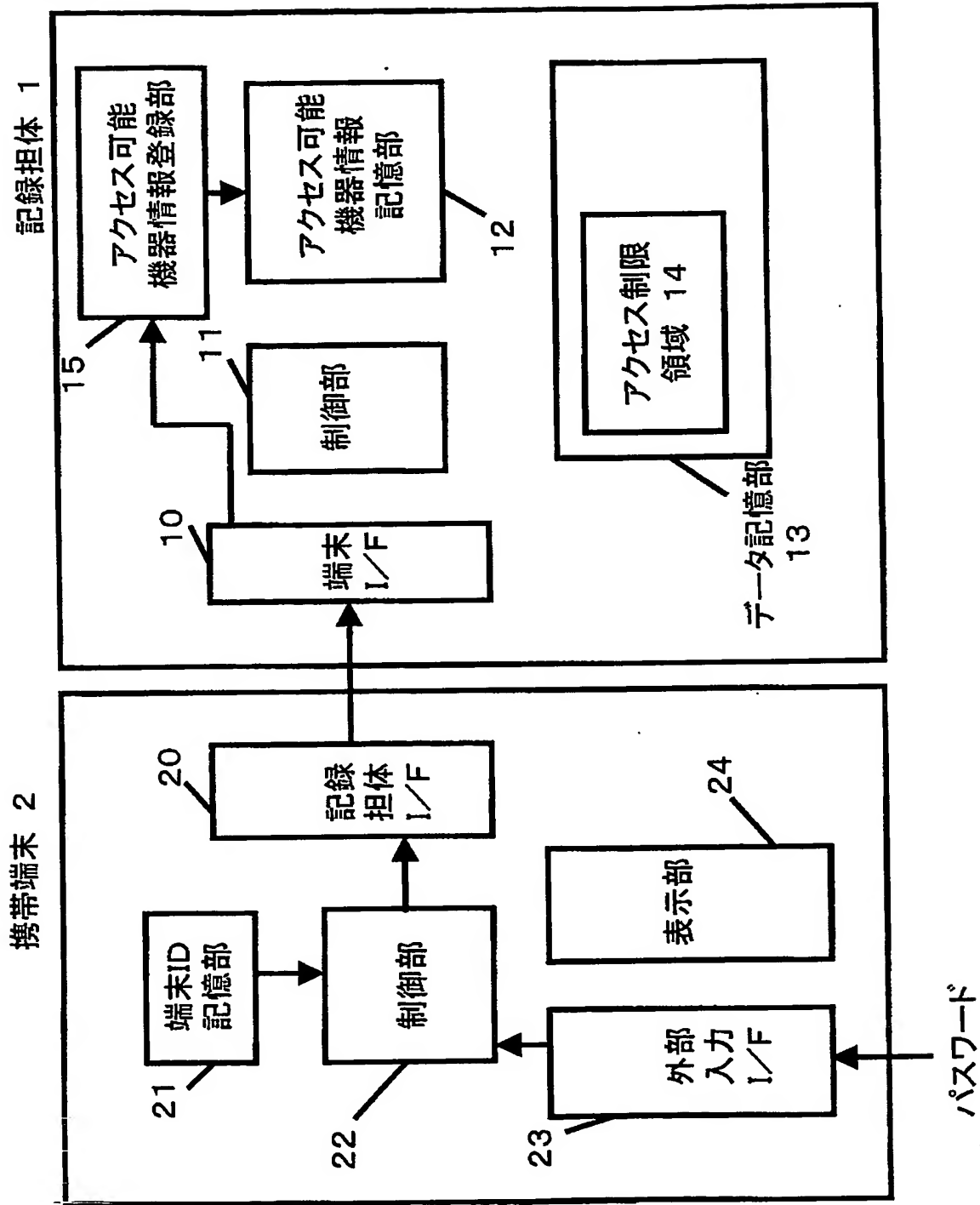
【書類名】 図面
【図 1】



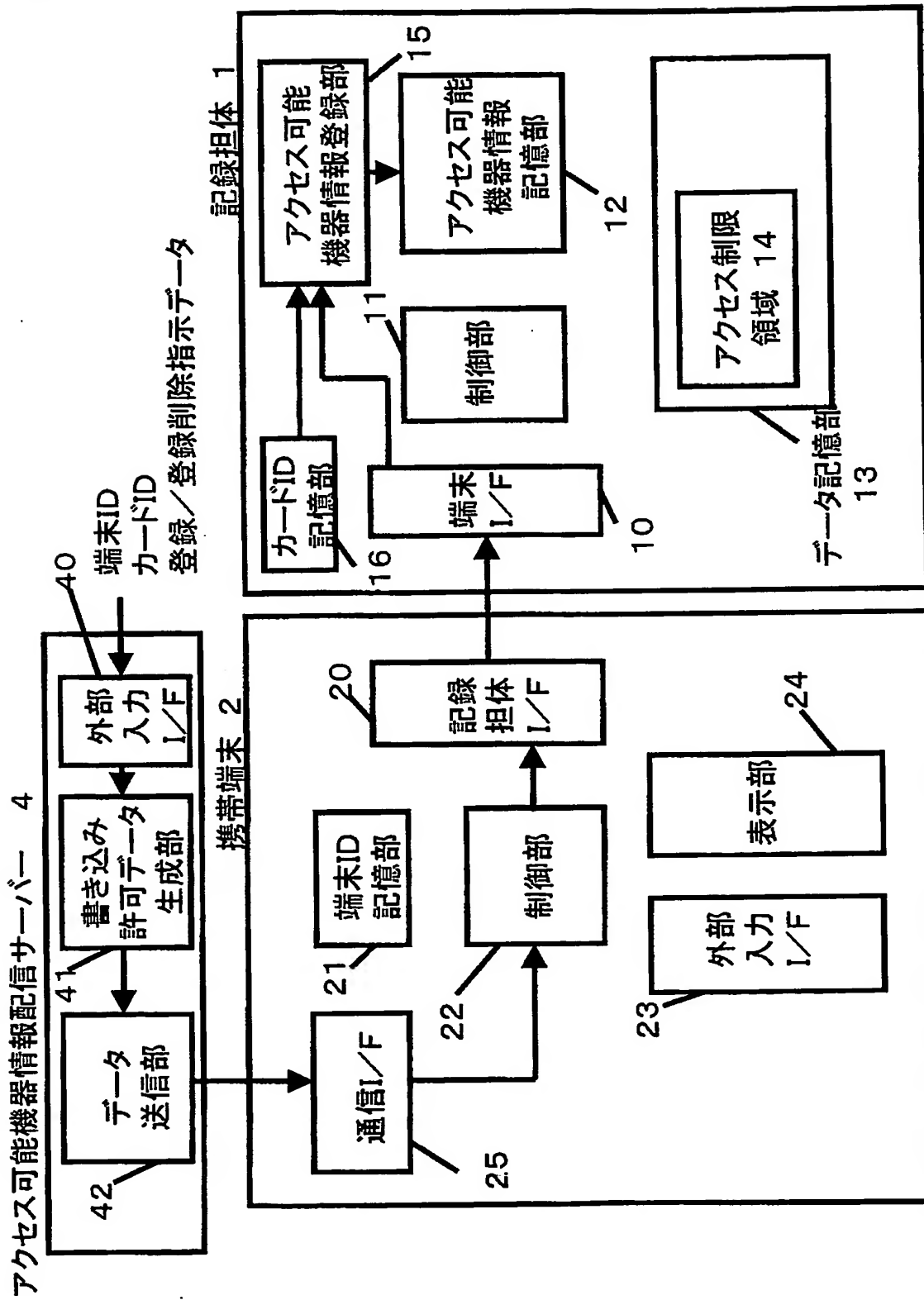
【図2】



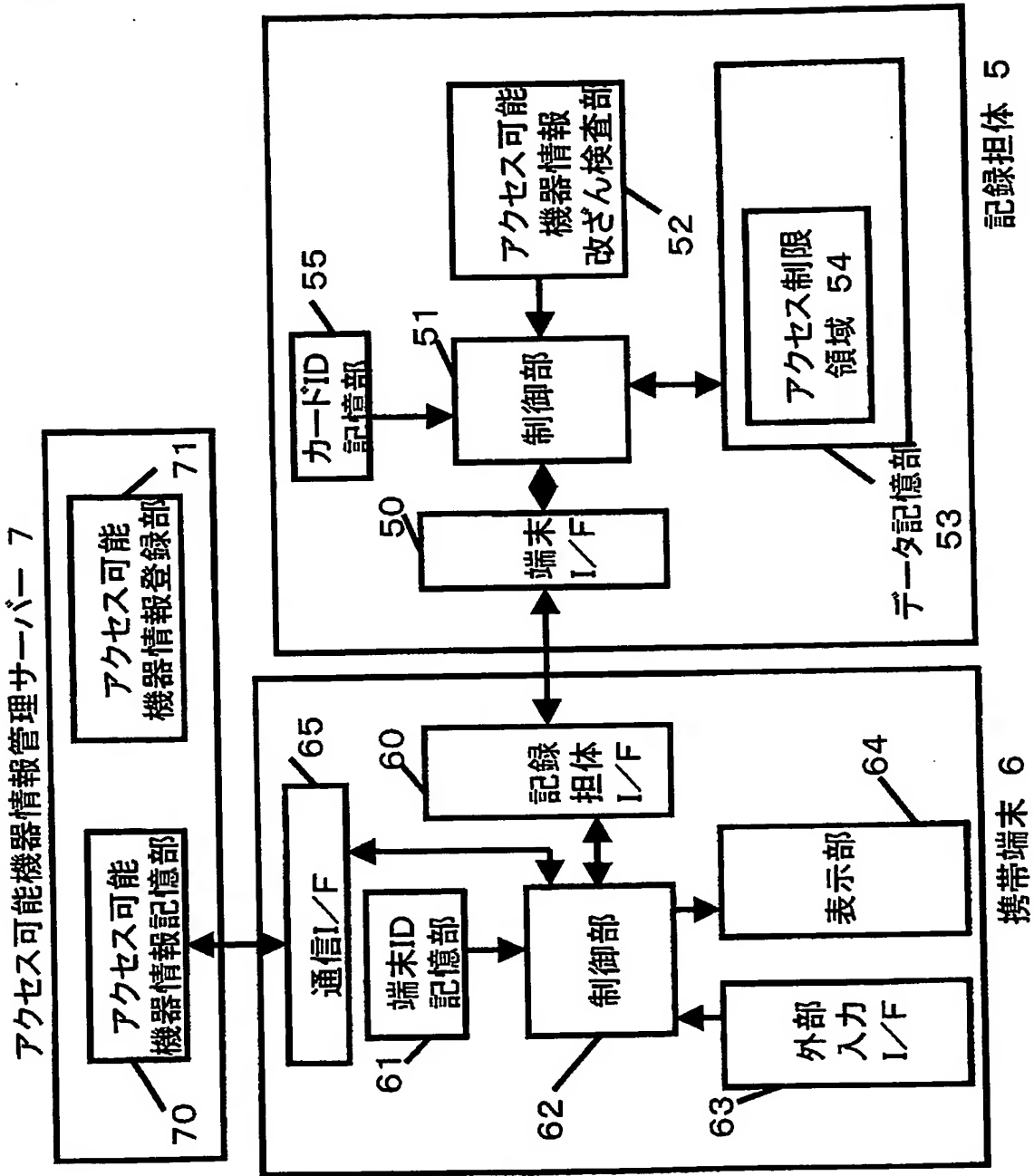
【図 3】



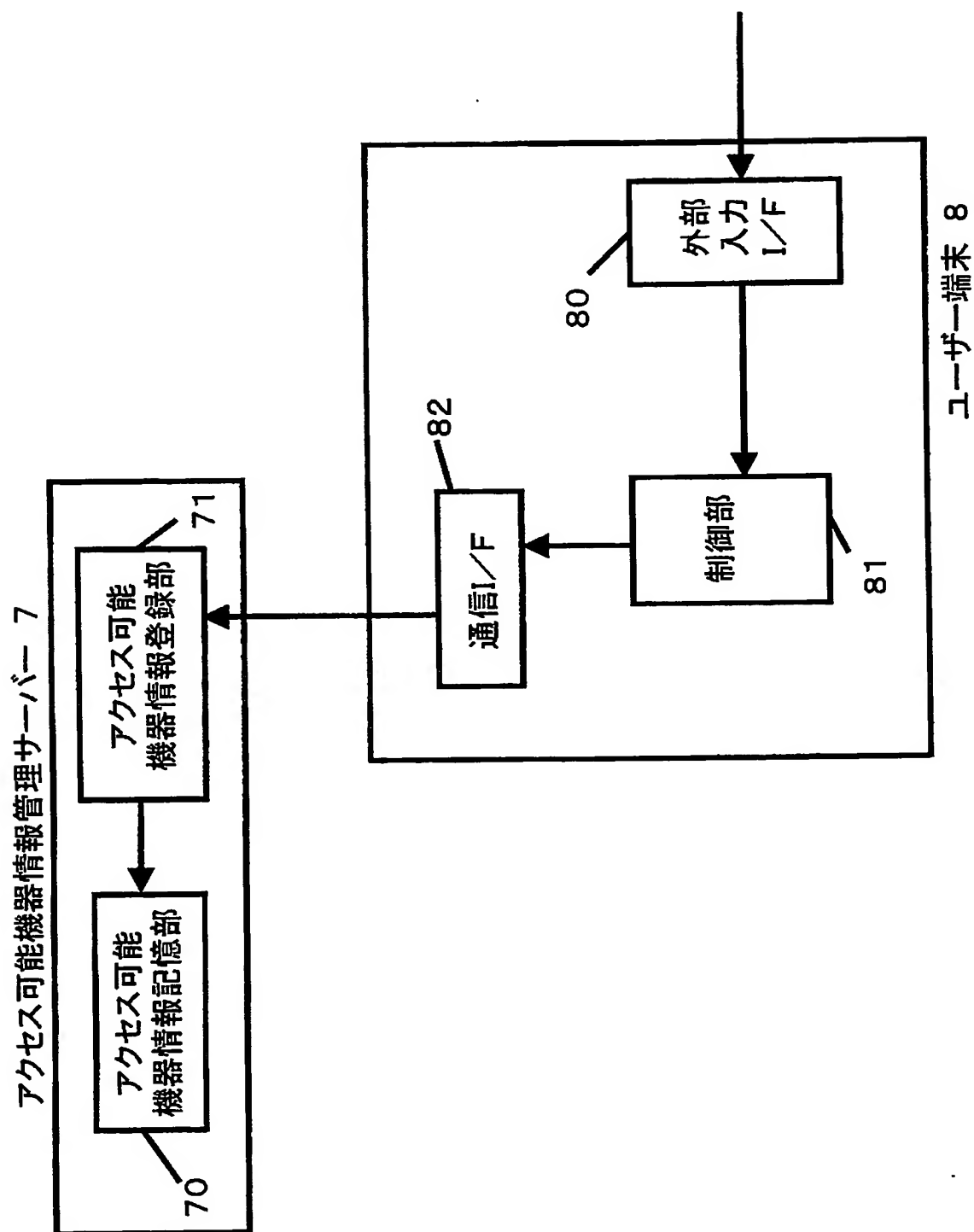
【図 4】



【図5】



【図 6】



【書類名】要約書

【要約】

【課題】メモリカード盗難時に、記憶内容の不正読み取りを防止すること。

【解決手段】メモリカード内に、アクセス可能な端末の端末IDリストを格納する手段と、それに基づいて端末からのアクセスの許可／不許可を判断する手段とを備えることによって、アクセス許可されていない端末によるメモリカード読み取りを防止し、正規カード保有者にとって操作の面で大きな負担をかけず、かつ、オフライン環境下でのカード内データの覗き見も防止することができる。

【選択図】図1

特願 2 0 0 3 - 3 5 6 0 7 2

出 願 人 履 歴 情 報

識別番号

[0 0 0 0 0 5 8 2 1]

1. 変更年月日

1 9 9 0 年 8 月 2 8 日

[変更理由]

新規登録

住 所

大阪府門真市大字門真 1 0 0 6 番地

氏 名

松下電器産業株式会社